1350.40 Access Control Criteria for Right to Use Automated Information Resources
Issued Date: August 18, 2006

SUBJECT: Access Control Criteria for Right to Use Automated Information Resources.

APPLICATION: This procedure applies to all Executive Branch Departments, Agencies, Boards or Commissions using State information technology resources including, but not limited to, networks, systems, computers, databases, and applications.

PURPOSE: To establish, document, and manage the allocation of user access rights for individuals accessing State of Michigan information technology resources to prevent inadvertent and inappropriate access to resources not authorized for the individual user and enhance the safeguarding of protected information, information and data systems, and other information technology resources of the State of Michigan by establishing a requirement to use one or more prescribed access controls.

CONTACT AGENCY: Department of Information Technology (DIT)
Office of Enterprise Security

TELEPHONE: 517/241-4090

FAX: 517/241-2013

SUMMARY: Access to State-protected information systems and computing resources will be based on each properly identified and named user's specific access privileges. Access to State of Michigan networks and protected resources will be strictly managed, controlled, and periodically reviewed and audited to ensure only authorized users gain access based on the specific privileges granted.

APPLICABLE FORMS: None

PROCEDURES:

A. Access to Public Information.

1. Read-only access to public (including information accessible as a public record defined in the Freedom of Information Act, MCL 15.231 et. seq.) or openly available information does not require the use of identification, authentication, authorization, or the application of intricate access control techniques or technologies.
2. Appropriate protective measures must be implemented only to safeguard the accuracy and integrity of available public information, applications, and data.
   a. Dissemination servers for State information classified "public" must have protection from unauthorized modification from internal risks and external denial of service attacks.
3. Information designated as public must be segregated from all non-public protected resources in specially designated public domain resource configurations whenever possible to reduce management complexity and decrease risk to protected resources.

B. Access to Protected Information.

1. All data not meeting the description of A.1., above, is classified as protected data and/or data fitting privacy protection legislation, or is personally identifying information that requires access controls.

2. Computer systems, applications, and data resources of Executive Branch agencies shall utilize all available approved technical mechanisms, administrative, and operational processes within a comprehensive access control strategy that protects the confidentiality, integrity and availability of the hosted systems, software, applications, and data.
    a. Appropriate measures are to be used to protect any confidential personal identifying information keyed into, and processed by a public system, such as a request form, comment form, or questionnaire.
    b. All protected digital information must be protected via access controls and privileges to prevent improper disclosure modification, deletion, or otherwise rendered unavailable.
    c. Protected information or data will be encrypted during the transmission and collection process and securely stored.
    d. Access to the public systems, data, and applications does not allow unauthorized access directly to networks or systems connected containing State information classified as protected.
3. Access to protected information and resources requires that the right to use, (read, modify, add, delete) be established on a strict business or operational need basis.
4. Access controls may include the use of technical or procedural mechanisms either enforced individually or in any combination of directories, access control lists and databases, operating systems, applications used in concert with individual user identification, group memberships, physical locations, organizational roles, tokens, or other variable factors such as time.
5. Access to protected information and computing processes shall be controlled and managed on the basis of a combination of State business unit needs and all applicable enterprise security policies and standards.
6. Management of access to networks, operating systems and files, application software, databases, dial-up or VPN access, or wireless mobile computing services will be based on by-name association of the user to identified access rights to ensure that only identified authorized users gain authenticated access to protected resources.

C. Access Control Methods and Management

1. Access controls are to be applied at all tiers appropriate to the zones and domain(s) providing the access path. All applications are to have some form of end-user access controls unless designated as an open public access resource.
    a. The granularity of the access privileges will vary by operating system and application platform.
    b. The greatest granularity available must be the foundation for management of access privileges.
2. Access controls must be managed through organizing access privileges in ways to ensure that even legitimate users cannot access nearby stored information unless they are authorized to do so.
3. Access control management must include the following considerations:
    a. Role based access controls are the minimum that must be applied to databases, applications, or computer hosts that contain protected information.
    b. System or application administrative privileges must be required to change the access control configuration on systems containing protected information.
    c. Access control must be modified when an individual's role changes within the organization within forty-eight hours or less.
    d. Policies controlling who gets access to which types of data must be clearly documented and reviewed on a regular basis by the business unit responsible for the underlying business process, application, or data.

e. Access control overrides are permitted during emergency situations. Conditions under which emergency overrides are allowed must be clearly documented along with who may authorize such overrides.
f. As a major component of access control, password and credential administration shall be managed to provide sufficient password security for the risk and severity level associated with the subject resource.
g. System utilities or operating system management controls should be available to only those users who have a business case for accessing the specific function. Access to program source libraries on production systems should be protected to ensure access by only authorized users. The operating system files and application software should be secured from unauthorized use or access.
h. When needed, access controls shall include restrictive time and date configurations that limit when connections will be allowed.
i. Passwords when used as a primary means to provide controlled access to resources must be selected, used, and managed to protect against unauthorized discovery or usage.
j. Each individual user will be limited by specific controls restraining the rights to 'read', 'write', 'execute', and 'delete' based on ownership of the information. Where resource ownership is shared, the rights to modify or write to files by individuals should be based on a business decision of the agency management and not on defaults in system settings.
k. Any State of Michigan computing resource should be configured to provide protection from unauthorized access to any application or utility that can override application or system access controls.
l. Any system should be sufficiently secured and configured to prevent compromising the applications or data of other systems with which it shares resources or communications.
m. Any system configuration should be able to limit access to information to only the owner of that information; other properly designated users, or defined groups of users, or associated system applications.
n. Access to "system help' that would provide information on how to override existing security measures should be restricted to authorized resource administrators.
o. Additional controls should exist to limit the ability of the user to display, transmit, or use the output of any application only in ways approved by the agency business management.

4. Access to systems containing protected information resources must be managed based on one or multiple selections of the alternative access control methods (defined at the end of this procedure) listed below in (a.) to (i.):
   a. UBAC (User Based Access Control)
   b. RBAC (Role Based Access Control)
   c. PBAC (Policy Based Access Control) aka. RSBAC (Rule Set Based Access Control)
   d. CDAC (Content Dependent Access Control)
   e. CBAC (Context Based Access Control)
   f. VBAC (View Based Access Control)
   g. TBAC (Time Based Access Control)
   h. PLAC (Physical Location Access Control)
   i. NNAC (Network Node Access Control)
   j. MAC (Mandatory Access Controls)
   k. DAC (Discretionary Access Controls)

D. Agency Responsibilities

1. Conduct a risk assessment to identify the data or resource risk and severity prior to establishing the level and selection of access controls to State of Michigan information systems and resources in accordance with current policy and published standards.
2. Designate users having access to specific applications based on business access control policy as formed by the agency business unit and the data security requirements profile.
    a. Access privileges established for access to protected information, data, or files shall be granted to named users and groups only on the basis of specific business need (i.e. a "need to know" basis).
    b. The owner of the system, application, or business process or his or her in-writing designee must authorize user access or delegate to others an operational process for authorizing access privileges.
    c. Access to any application containing protected data should be denied by default unless a need for access can be demonstrated and is documented.
3. Establish internal administrative procedures to ensure that the functionality, connectivity, and services supported by information systems restrict users' privileges based on requirements related directly to their job function.
4. Ensure that the use of remote or telecommuting facilities meets the same security standards as normal internal facilities.
5. Provide copies of State security policies to third parties requiring access and require compliance with the security policies by contract.
6. Positively identify all users prior to granting ability to use any protected resources.
7. Promptly report all significant changes in end-user duties or employment status to the appropriate security administrator handling the user-IDs of the affected persons.
8. Promptly terminate all State information systems privileges at the time that a worker, vendor, contractor, agent, or volunteer ceases to provide services to the State of Michigan.
9. Manage and document all stages in the life cycle of user access; from the initial registration of new users to the final de-registration of users who no longer require access to State of Michigan information systems and resources.

E. End User Responsibilities, including Third Parties

1. Users, regardless of their status or category, have the responsibility to safeguard primary means of access to State protected resources that are entrusted to them as well as take measures to safeguard physical access to secondary reproductions in digital media or hard copy format.
    a. When contract personnel are working in a State environment without being directly supervised then State employees must be vigilant about logging off sessions, logging out or securing PC access, and keeping paper information properly discreet.
2. End users, with consent from their business process manager or supervisor, may use DAC (Discretionary Access Controls) on local files provided that the approving supervisor can also access any critical single-copy business resource files.
3. Third parties' access into State resources falls into two primary categories.
    a. Physical Access.
        i. Contractor working on State premises unrelated to computing resources but State computing resources are physically co-located. Contractor must not use the computing resources.
        ii. Contractor working directly on the computing systems and granted user account. Contractors having user accounts on State systems must meet and follow the same standards as regular State employees.
    b. Logical Access.
        i. Access of State resources via external method such as a remote dial-in or a connection through a firewall or even a login through a direct network connection.
        ii. Logical access may present a very cost effective way of using third party resources; however it presents a significant risk in that it is more difficult

to monitor the actions of the third party. Very tight controls should be required on user accounts using remote logical access.

iii. In situations where a firewall is not technically feasible, DIT security administration must be involved in actively monitoring the connection to determine if abnormal activity is taking place.

F. DIT responsibilities:

1. Manage the access procedures using the following life cycle steps.
   a. Identity verification
   b. Enrollment
   c. Routine use
   d. Transaction management
   e. Records management
   f. Testing
   g. Suspension, revocation, & re-issuance
   h. Audit
   i. De-registration, or termination
2. Not grant access privileges to any user without specific written approval from the Agency information owner.
3. Issue user ID and related password.
4. Implement the technical requirements for granting access rights or privileges.
5. Terminate, change or de-commission user ID, password and/or access within 48 hours of receipt of request by Agency.
6. Certify fully functioning implementation of access as authorized.
7. Certify compliance with established IT security policies, standards and procedures.
8. Through DIT Office of Enterprise Security, review and monitor procedure to ensure appropriate authorization methods are implemented and take actions necessary to ensure compliance with State of Michigan IT security policies, standards, and procedures.
9. Through Internal Auditor, conduct periodic audits of IT resources, including third party systems for appropriate controls to maintain compliance with policy and standards.
   a. Alternately, a contracted security firm may be used to examine off-site third party systems and provide a determination that the third party site presents no additional risk of loss for State of Michigan resources.

G. State agencies desiring to implement practices and procedures differing from this procedure may do so only with the written approval of the DIT Office of Enterprise Security.

H. Definitions:

UBAC (User Based Access Control) – defining permissions for each user, also called identity based access control.

RBAC (Role Based Access Control) – uses a profile to map a group of users to resources.

PBAC (Policy Based Access Control) – is a set of rules that determine access rights.

a.k.a. RSBAC (Rule Set Based Access Control) – is a set of rules that determine access rights.

CDAC (Content Dependent Access Control) – limits the rights of users based on content of resource to specific fields (range) or cells (data point) typically within a database.

CBAC (Context Based Access Control) – includes sequence of events that preceded the access attempt to grant or deny access.

VBAC (View Based Access Control) – uses predefined interfaces (views) so that users only gain access to sub-resources within allowed view.

TBAC (Time Based Access Control) – limits access to resources based on time associations.

PLAC (Physical Location Access Control) – limits access to resources by a given location.

NNAC (Network Node Access Control) – limits access to specific nodes or networks.

MAC (Mandatory Access Controls) – are required controls.

DAC (Discretionary Access Controls) – are optional to the user to use or not use.

Authority is The Management and Budget Act, Public Act 431 of 1984, as amended, § 203.

* * *